SEWP Security Center Open House, June 29, 2005

Our Mission**:** *Working to provide IT security experience and tools to SEWP Partners in the Federal Government*

Background—Computer security is more than viruses, worms, trojans, subversion, reconnaissance, intrusions, compromise, Spam, spyware, rootkits, and social engineering. Computer security is about applying standard business process in the form of Risk Management to security problems. The process of Risk Management includes: identifying assets, considering vulnerabilities, considering threats, and then valuating risk as the product of threats and vulnerabilities. Once risk has been valuated then it can either be accepted (an acceptable risk), transferred (buy insurance), or mitigated (lower the risk level).

Traditional approaches to security risk mitigation include *defense-in-depth* and *time-based security*. Defense-in-depth is a layered security approach—where no single breach of security should result in a total failure (compromise). An example of this approach is a castle protected by walls, moats, and ramparts. Time-based security considers that a system or component only has to last (stay secure) until the alarm is sounded and help arrives. Safes are rated as TL-*nn*, for instance, where *nn* is the number of minutes that the safe will resist compromise (by blunt force, drill, or torch).

The primary way to consider mitigation is by considering the goals of computer security, CIA+AAA (confidentiality, integrity, availability + authentication, authorization, and auditing). To improve upon these components of computer security, the Security Center is interested and involved in a number of areas.

IdM—The SEWPSC has been working in the area of Identity Management (IdM) for the past several years. The combination of userid and password is by far the most widely used method of authentication. The goal of IdM is to reduce the requirements for users to maintain multiple passwords to access multiple systems. Besides reducing password maintenance for users (single sign-on, one password for all systems) authentication can be strengthened by requiring more than one form of identification (password and either a card, token, or a biometric reading). The SEWPSC hosted a Symposium on Identity Management in June, 2004. We were able to attract two world class keynote speakers to this event: Whitfield Diffie, the father of modern cryptography, and Kevin Mitnick, former hacker and the premier expert on social engineering. This event was well attended and rated highly successful.

The SEWPSC is also working with the Open Group, a leading industry standards organization, on Identity Management. We are endeavoring to catalog the 50 or so companies that provide solutions in the IdM space. This catalog will provide for a comparison of features and technologies supported by the products. The catalog will hopefully be a starting point to host demonstrations of compatibility amongst the different vendors.

over…

…continued

FIPS 201—This standards document from NIST defines the requirements of integrating physical and logical security (access to buildings and access to computers) through the use of a smart card (a credit card sized device that includes integrated cryptographic electronics). FIPS 201 also mandates aggressive implementation and deployment of this smart card starting in September, 2005. The SEWPSC has developed a FAQ for this document. By using a FAQ format to answer 45 questions, we directly point out the salient features and provide numerous links and references to the supporting standards. We are also interested in the second phase of this requirement (PIV-2) which will require PKI (Public Key Infrastructure) authorities to federate—PKI federation has long been a difficult endeavor.

NGSCB and Hardware Based Security—NGSCB was an attempt by Microsoft to significantly change the methods of security by utilizing new hardware (primarily a TPM), which is now embedded in most new PCs. NGSCB offered several new features including *attestation*. Attestation allows for strong reliability of integrity at end-points of distributed systems (perhaps the first real measure of reliability among distributed systems). Due to application implementation complexity most NGSCB features have been removed from the next release of Windows (Longhorn). The TPM will still be utilized to protect the hard drive in Longhorn (the secure start-up feature). Please see our presentation from SANS World Conference 2004 for a detailed description of NGSCB.

The TPM is based upon open specifications developed by the Trusted Computing Group. The TPM may shortly be employed in a number of network access protection mechanisms. These mechanisms protect inside perimeter machines from malware by denying infected machines access to the network. Machines are isolated at startup and initial connection until presenting evidence, usually from an anti-virus program, that they are not infected. Cisco's NAC (Network Admission Control) and Microsoft's forthcoming NAP (Network Access Protection) provide this form of protection. The SEWPSC is most interested in an open specification for protected network connection called TNC (Trusted Network Connect) from the TCG. In the long range the SEWPSC hopes such work can lead to a means for attestation of authentication protocols.

Spam—The most typical and perhaps most annoying security breach. The SEWPSC is interested in the Sender-ID Framework and SPF. Upcoming releases of Sendmail and Exchange (Exchange 2003 via Service Pack 2) promise to support these standards. These technologies work by using DNS to authorize (and be responsible for) which hosts are eligible to originate mail. The SEWPSC is planning to pilot an interoperability test of mail transfer using the Sender-ID capability between Exchange and Sendmail.